



**‘Know Your Customer (KYC),  
Anti Money Laundering (AML),  
Combating Financing Terrorism (CFT)  
&  
Maintenance of Deposit Accounts’ Policy**

**THE JANATA CO-OPERATIVE BANK LTD.**

H.O.32, Netaji Subhash Marg, Darya Ganj, New Delhi-110 002

Telephones : 23256272-74, E-mail : ho-manager@janatabank.in

<b>S.No.</b>	<b>Topic Area</b>	<b>Page #</b>
1	Objective	1
2	Scope and applicability	1-2
3	Definitions	3-7
4	Know Your Customer Policy	7
5	Money Laundering and Terrorist Financing Risk Assessment by Bank	7-8
6	Designated Director	8
7	Principal Officer	8-9
8	Compliance of KYC policy	9
9,10, 10A	Customer Acceptance Policy	9-10
11	Risk Management	10-12
12	Customer Identification Procedure (CIP)	12-13
13	Customer Due Diligence (CDD) Procedure	13-14
14	Accounts opened using OTP based e-KYC	15-16
15	V-CIP	16-20
16	KYC verification	20
17	Customer Due Diligence (CDD) Measures for Sole Proprietary firms	20-21
18	CDD Measures for Legal Entities	21-24
19	Identification of Beneficial Owner	24
20	On-going Due Diligence	24
21	Extent of Monitoring	24-25
22	Monitoring Operations	25-26
23	Periodic Updation of KYC	26-28
24	Existing Customers	28
25	Enhanced and Simplified Due Diligence Procedure	28-30
26	Record Management	30-31
27	Reporting Requirements to Financial Intelligence Unit - India	31-37
28	Requirements/obligations under International Agreements	37-38
29,30, 30A	Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005)	38-39
31,31A	Jurisdictions that do not or insufficiently apply the FATF	39
32	Secrecy Obligations and Sharing of Information	40

33	CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)	40-41
34	Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)	41-42
35	Period for presenting payment instruments	42
36	Operation of Bank Accounts & Money Mules	42
37	Collection of Account Payee Cheques	42
38	Unique Customer Identification Code (UCIC)	42
39	Introduction of New Technologies – Credit Cards/Debit Cards/ Smart Cards/Gift Cards/Mobile Wallet/Net Banking/Mobile Banking/RTGS/NEFT/ ECS/ IMPS etc.	42
40	Correspondent Banks	43
41	Wire Transfer	43
42	Issue and Payment of Demand Drafts, etc.,	43
43	Quoting of PAN	44
44	Selling Third party products	44
45	At-par cheque facility	44
46	Hiring of Employees and Employee training	45
47	Penalty for non compliance	45-46
48	Conclusion.	46
49	Annex - I	47-53
50	Annex - II	54-56

# **THE JANATA CO-OPERATIVE BANK LTD.**

**H.O.32, Netaji Subhash Marg, Darya Ganj, New Delhi-110 002**

**Telephones : 23256272-74, E-mail : ho-manager@janatabank.in**

## **‘Know Your Customer (KYC), Anti Money Laundering (AML), Combating Financing Terrorism (CFT) & Maintenance of Deposit Accounts” Policy**

The ‘Know Your Customer (KYC), Anti Money Laundering (AML), Combating Financing Terrorism (CFT) & Maintenance of Deposit Accounts” Policy of the bank in vogue has been reviewed in accordance with the RBI Directives on Know Your Customer (KYC) updated up to May 4, 2023 recommended by the Inspection and Audit Compliance Sub-Committee and approved by the BoM/Board in its meeting held on 20/09.2023/26.09.2023 vide Resolution No.A1.(e)(ii) as under :

### **1. Objectives**

The Objective of KYC guidelines is to prevent the bank from being used, intentionally or unintentionally, by criminal elements for money laundering activities. Bank is required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions. Bank shall take steps to implement the provisions of the aforementioned Act and Rules, including operational instructions issued in pursuance of such amendment(s). It will also enable the bank to know our customers and their financial dealings better, which in turn will help the bank to manage its risks prudently. This KYC Policy has been framed to develop a strong mechanism for achieving the following objectives :

- i. To prevent Bank from being used intentionally or unintentionally, by criminal elements for Money Laundering or Terrorist Financing activities. KYC procedures also enable the Bank to know/understand their customers and their financial dealings better, which in turn helps it to manage the associated risks prudently.
- ii. To enable the Bank to comply with all the legal and regulatory obligations in respect of KYC norms/AML standards /CFT measures/Bank’s Obligation under PMLA, 2002 and to cooperate with various government bodies dealing with related issues.
- iii. The purpose of KYC policy is to put in place customer identification procedures for opening of accounts and monitoring transactions in the accounts for detection of transactions of suspicious nature for the purpose of reporting to Financial Intelligence Unit-India [FIU-IND] in terms of the recommendations made by Financial Action Task Force (FATF) and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision (BCBS) on AML standards and on CFT measures.
- iv. For this Policy, the term ‘Money Laundering’ would also cover financial transactions where the end-use of funds is for financing terrorism, irrespective of the source of funds.

### **2. Scope and applicability**

#### **A. Scope and applicability of KYC Policy of the Bank**

All branches of the Bank shall take all necessary steps to implement this KYC policy and provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money- Laundering (Maintenance of Records) Rules, 2005, as amended from time to time, including operational

instructions issued in pursuance of such amendment(s). The provisions of KYC Policy guidelines shall apply to all the branches of the Bank.

Bank's policy framework shall seek to ensure compliance with PML Act/Rules, including regulatory instructions in this regard and should provide a bulwark against threats arising from money laundering, terrorist financing, proliferation financing and other related risks. While ensuring compliance of the legal/regulatory requirements as above, it shall also be considered to adopt best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.

## **B. Policy contents**

**The KYC policy includes following key elements :**

### **Customer Acceptance Policy**

Bank's Customer Acceptance Policy (CAP) lays down the guidelines for acceptance of customers. It is to be ensured as under: -

- (i) No account is opened in anonymous or fictitious / benami name.
- (ii) No account is opened where the Bank is unable to apply appropriate Customer Due Diligence (CDD) measures, either due to non-cooperation of the customer or non-reliability of the documents / information furnished by the customer.
- (iii) No transaction or account based relationship is undertaken without following the CDD procedure.
- (iv) The mandatory information sought for KYC purpose while opening an account and during the periodic updation, is specified.
- (v) Additional information, where such information requirement has not been specified in KYC Policy of the Bank, is obtained with the explicit consent of the customer.
- (vi) The CDD procedure is to be applied at the Unique Customer Identification Card level. Thus, if an existing KYC compliant customer of Bank desires to open another account with the same Bank, there shall be no need for a fresh CDD exercise.
- (vii) CDD Procedure is followed for all the joint account holders, while opening a joint account.
- (viii) Circumstances in which, a customer is permitted to act on behalf of another person / entity, are clearly spelt out.
- (ix) No account is opened where identity of the customer matches with any person or entity, whose name appears in the sanctions lists indicated in Chapter IX of the Master Direction of RBI last updated upto 04.05.2023.
- (x) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

Where Goods & Services Tax (GST) details are available, the GST number shall be verified from the search/ verification facility of the issuing authority.

- C. It is to be ensured that the Customer Acceptance Policy shall not result in denial of banking / financial facility to members of the general public, especially those, who are financially or socially disadvantaged.
- D. Where a suspicion of money laundering or terrorist financing, is formed and reasonably believed that performing the CDD process will tip-off the customer, CDD process shall not be pursued, instead it shall be reported to Head Office for onward submission of STR to FIU –IND.

### 3. Definitions

In these Directions, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:

- A. Terms bearing meaning assigned in terms of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005:
- i. Aadhaar number", as defined under sub-section (a) of section 2 of the *Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016*, henceforth 'The Aadhaar Act', means an identification number issued to an individual by Unique Identification Authority of India (UIDAI) on receipt of the demographic information and biometric information as per the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
  - ii. "Act" and "Rules" means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.
  - iii. "Authentication", as defined under sub-section (c) of section 2 of the Aadhaar Act, means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository (CIDR) for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it;
  - iv. **Beneficial Owner (BO)**
    - a) Where the **customer is a company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.  
Explanation- For the purpose of this sub-clause-
      - (i) "**Controlling ownership interest**" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company.
      - (ii) "**Control**" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.
    - b) Where the **customer is a partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.
    - c) Where the **customer is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.
    - d) Where the **customer is a trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.
  - v. "**Certified Copy**" - Obtaining a certified copy by the Bank shall mean comparing the copy of

the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the Bank as per the provisions contained in the Act.

- vi. **“Central KYC Records Registry”** (CKYCR) means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.
- vii. **“Designated Director”** means a person designated by the bank who holds the position of senior management or equivalent designated as a 'Designated Director' to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include:-
- e) a person who holds the position of senior management or equivalent designated as a 'Designated Director' in respect of the Bank.
- viii. **“Digital KYC”** means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the bank as per the provisions contained in the Act.
- ix. **“Digital Signature”** shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).
- x. **“Equivalent e-document”** means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.
- xi. **“Group”** - The term “group” shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act, 1961 (43 of 1961).
- xii. **“Know Your Client (KYC) Identifier”** means the unique number or code assigned to a customer by the Central KYC Records Registry.
- xiii. **“Non-profit organisations”** (NPO) means any entity or organisation that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013.
- xiv. **“Officially Valid Document”** (OVD) means the passport, the driving licence, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, letter issued by the National Population Register containing details of name and address.

Provided that,

- a) where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
- b) where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-
- (i) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

- (ii) property or Municipal tax receipt;
- (iii) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
- (iv) letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;

- c) the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above
- d) where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

xv. "**Offline verification**" shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

xvi. "**Person**" has the same meaning assigned in the Act and includes:

- a) an individual,
- b) a Hindu undivided family,
- c) a company,
- d) a firm,
- e) an association of persons or a body of individuals, whether incorporated or not,
- f) every artificial juridical person, not falling within any one of the above persons (a to e), and
- g) any agency, office or branch owned or controlled by any of the above persons (a to f).

xvii. "**Principal Officer**" means an officer nominated by the bank, responsible for furnishing information as per rule 8 of the Rules.

xviii. "**Suspicious transaction**" means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith,:

- a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
- b) appears to be made in circumstances of unusual or unjustified complexity; or
- c) appears to not have economic rationale or *bona-fide* purpose; or
- d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.



- xix. A '**Small Account**' means a savings account in which:
- a) the aggregate of all credits in a financial year does not exceed rupees onelakh;
  - b) the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and
  - c) the balance at any point of time does not exceed rupees fifty thousand.

Provided, that this limit on balance shall not be considered while making deposits through Government grants, welfare benefits and payment against procurements.

- xx. "**Transaction**" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:
- a) opening of an account;
  - b) deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
  - c) the use of a safety deposit box or any other form of safe deposit;
  - d) entering into any fiduciary relationship;
  - e) any payment made or received, in whole or in part, for any contractual or other legal obligation; or
  - f) establishing or creating a legal person or legal arrangement.
- xxi. Video based Customer Identification Process (V-CIP)": a method of customer identification by an official of the bank by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer. Such process shall be treated as face-to-face process for the purpose of this Master Direction.

B. Terms bearing meaning assigned in this Directions, unless the context otherwise requires, shall bear the meanings assigned to them below:

- i. "**Common Reporting Standards**" (CRS) means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.
- ii. **Correspondent Banking:** Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Respondent banks may be provided with a wide range of services, including cash management (e.g., interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.
- iii. "**Customer**" means a person who is engaged in a financial transaction or activity with a bank and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
- iv. "**Walk-in Customer**" means a person who does not have an account based relationship with the bank, but undertakes transactions with the bank.
- v. "**Customer Due Diligence (CDD)**" means identifying and verifying the customer and the beneficial owner.
- vi. "**Customer identification**" means undertaking the process of CDD.
- vii. "**FATCA**" means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.

- viii. **“IGA”** means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.
- ix. **“KYC Templates”** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
- x. **“Non-face-to-face customers”** means customers who open accounts without visiting the branch/offices of the bank or meeting the officials of bank.
- xi. **“On-going Due Diligence”** means regular monitoring of transactions in accounts to ensure that they are consistent with the customers’ profile and source of funds.
- xii. **Payable-through accounts:** The term payable-through accounts refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.
- xiii. **“Periodic Updation”** means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.
- xiv. **“Politically Exposed Persons”** (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.
- xv. **“Bank”** means  
The Janata Co-operative Bank Ltd. and its branches/offices
- xvi. **“Wire transfer”** means a transaction carried out, directly or through a chain of transfers, on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank.
- xvii. **“Domestic and cross-border wire transfer”**: When the originator bank and the beneficiary bank is the same person or different person located in the same country, such a transaction is a domestic wire transfer, and if the ‘originator bank’ or ‘beneficiary bank’ is located in different countries such a transaction is cross-border wire transfer.
- C. All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act or the Reserve Bank of India Act, or the Prevention of Money Laundering Act and Prevention of Money Laundering (Maintenance of Records) Rules, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

#### 4. Know Your Customer Policy

The KYC policy shall include following four key elements:

- a. Customer Acceptance Policy;
- b. Risk Management;
- c. Customer Identification Procedures (CIP); and
- d. Monitoring of Transactions

#### 5. Money Laundering and Terrorist Financing Risk Assessment by Bank :

- i. Bank shall carry out ‘Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment’ exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.
- ii. The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, Bank shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with banks from time to time.

- iii. The risk assessment by the bank shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/ structure, etc. of the bank. Further, the periodicity of risk assessment exercise shall be determined by the Board of the bank, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.
- iv. The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated, and should be available to competent authorities and self-regulating bodies.
- v. Banks shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, Banks shall monitor the implementation of the controls and enhance them if necessary.

#### **6. Designated Director:**

The Managing Director/Chief Executive Officer of the Janata Co-operative Bank Ltd. is nominated as “designated Director”, as required under provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (Rules), to ensure compliance with the obligations under the Act and Rules. The name, designation and address of the Designated Director shall be communicated to the FIU-IND & Reserve Bank of India.

#### **7. Principal Officer:**

The Manager at Head Office of the bank is designated as Principal Officer (PO). The PO should be independent and report directly to the senior management or to the Board of Directors. The PO shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations. The name, designation and address of the Principal Officer may be communicated to the FIU-IND & Reserve Bank of India.

In the absence of the Manager Head Office the Assistant Manager at Head Office shall act a principal Officer and will be responsible for monitoring and reporting all the transactions as mentioned above.

#### **A. Appointment of Principal Officer**

The Manager at the Head Office will act as Principal Officer and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He/she will maintain close liaison with the enforcement agencies, banks and any other institution, which are involved in the fight against money laundering and combating financing of terrorism.

Duties of the Principal Officer will be as follows :-

- i. Over all monitoring of the implementation of Banks KYC/AML/CFT policy.
- ii. Monitoring and reporting of transaction and sharing of information as required under the law.
- iii. Interaction with Branch Manager for ensuring full compliance with the policy.
- iv. Timely submission of Cash Transaction Reports (CTRs). Suspicious Transaction Reports (STRs). Counterfeit Currency Reports (CCRs) and other related reports/returns to FIU-IND.
- v. Maintaining liaison with the law enforcing agencies, in fight against money laundering

and combating financing of terrorism.

- vi. Ensuring submission of periodical report to top management/Board.
- vii. Prompt reporting of information regarding suspicious transactions to the law enforcing authority concerned in consultation with Principal Officer in Head Office

## **B. Duties Responsibilities and accountability**

The chain of duties and responsibilities at branches/controlling offices and accountability are as under and non-compliance of the duties and responsibilities arising out of KYC guidelines will lead to fixation of accountability. Dereliction of duty and avoidance of knowledge will lead to examination of staff accountability.

Officer in Charge of accounts/ Officer vested with the authority to open new accounts;

To interview the potential customer

- i. To verify the introductory reference/ customer profile
- ii. To arrive at there should limits for each account (new as well as existing) and to exercise due diligence in identifying suspicious transactions.
- iii. To ensure against opening of accounts in the names of terrorist/banned organizations
- iv. To adhere to the provisions of Foreign Contribution Regulatory Act. 1976
- v. To comply with the guidelines issued by the bank from time in respect of opening and conduct of account.

## **8. Compliance of KYC policy**

- i) bank shall ensure compliance with KYC Policy through:
  - a) Specifying as to who constitute 'Senior Management' for the purpose of KYC compliance.
  - b) Allocation of responsibility for effective implementation of policies and procedures.
  - c) Independent evaluation of the compliance functions of bank policies and procedures, including legal and regulatory requirements.
  - d) Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures.
  - e) Submission of quarterly audit notes and compliance to the Audit Committee.
- ii. bank shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

## **9. Customer Acceptance Policy**

Without prejudice to the generality of the aspect that Customer Acceptance Policy may contain, bank shall ensure that :

- i. No account is opened in anonymous or fictitious/benami name.
- ii. No account is opened where the bank is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
- iii. No transaction or account based relationship is undertaken without following the CDD procedure.

- iv. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
  - v. 'Optional'/additional information, is obtained with the explicit consent of the customer after the account is opened.
  - vi. Bank shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of a banks desires to open another account with the same banks, there shall be no need for a fresh CDD exercise.
  - vii. CDD Procedure is followed for all the joint account holders, while opening a joint account.
  - viii. Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
  - ix. Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.
  - x. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
  - xi. Where an equivalent e-document is obtained from the customer, bank shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
- 10.** Customer Acceptance Policy shall not result in denial of banking/financial facility to members of the general public, especially those, who are financially or socially disadvantaged.
- 10.A** Where Bank forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND.

## **11. Risk Management**

A. For Risk Management, bank shall have a risk based approach which includes the following.

- i. Customers shall be categorised as low, medium and high risk category, based on the assessment and risk perception of the bank.
- ii. Broad principles may be laid down by the Bank for risk-categorisation of customers.
- iii. Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the clients' business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.
- iv. The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer

Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive and the same is specified in the KYC policy.

Explanation: FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), guidance note circulated to all cooperative banks by the RBI etc., may also be used in risk assessment.

B. Having formulated an effective KYC programme it is essential to ensure its proper implementation and also ensuring that Bank's policies and procedures are implemented effectively. The Branch Managers will implement the instructions conveyed to them by head office from time to time. The nature and extent of due diligence will depend on the risk perceived by Branch. The Principal Officer at Head Office will ensure proper implementation in branches under their control.

- i. Branches should prepare a profile for each new customer based on risk categorisation. The customer profile should contain information relating to customer's identity, social/financial status, nature of business activity, information about the clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the bank.
- ii. Branches should categorise their customers into low, medium and high risk category based on their assessment and risk perception of the customers, identifying transactions that fall outside the regular pattern of activity and not merely based on any group or class they belong to. The branches are advised to ensure that the policies are complied meticulously. The nature and extent of due diligence, may be based on the following principles:

Customers that are categorized as medium or high risk etc. Manger may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

For the purpose of customers profile of individual accounts holders the following information shall be collected at the time of opening of Account (already incorporated in the account opening form) Mandatory information :-

- a) Occupation
- b) Source of funds
- c) Monthly income
- d) Annual Turnover
- e) Date of Birth
- f) Dealing with other Banks
- g) Existing Credit facilities

Optional information for better customer relationship (already incorporated in account opening form)

- a) Marital status
- b) Educational Qualification
- c) Educational qualification of spouse
- d) Information regarding Children
- e) Ownership of car/two wheeler house etc.
- f) Having credit card
- g) Having insurance policy

### **Low Risk**

Individuals (other than High Net Worth) and entities, whose identity and source of income, can be easily identified, and customers in whose accounts the transactions conform to the known profile, may be categorised as low risk.

- a) Salaried employees
- b) People belonging to lower economic strata of the society whose accounts show small balances and low turn over.
- c) Accounts of members/member cooperative societies
- d) Reputed persons of the area as per information available in public.
- e) Small businessmen/retail traders of the area with turn over below Rs.10.00 Lacs per month.
- f) Small/marginal/other farmers who are native of the area.

### **Medium Risk**

Customers who are likely to pose a higher than average risk should be categorised as medium risk.

- a) Trusts/Charities/NGO's not receiving donations
- b) Businessmen/retail traders of the area with turn over of above Rs.10.00 Lacs per month.
- c) Accounts with frequent transactions in the form of issue/collection of cheque DD etc.
- d) Client accounts opened by a professional intermediary on behalf of client
- e) Any other account as may be perceived risky by the Manager.

### **High Risk**

High risk depending on the background, nature and location of activity, country of origin, sources of funds, customer profile, etc. Customers requiring very high level of monitoring, e.g., those involved in cash intensive business, Politically Exposed Persons (PEPs) of foreign origin, may, if considered necessary, be categorised as high risk.

- a) Non-resident customers
- b) High net worth individuals
- c) Trusts/Charities/NGO's and other organizations receiving donations.
- d) Companies having close family share holding or beneficial ownership.
- e) Firms with sleeping partners.
- f) Politically exposed persons (PEP) of foreign origin
- g) Those with dubious reputation as per public information available.
- h) Accounts of non-face to face customers.
- i) Any other account as may be perceived to be highly risky by the manager.

## **12. Customer Identification Procedure (CIP) :**

Customer identification means undertaking client due diligence measures while commencing an account-based relationship including identifying and verifying the customer and the beneficial owner on the basis of one of the OVDs. Banks need to obtain sufficient information to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of the banking relationship. The bank must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk-based approach is considered necessary to avoid disproportionate cost to the bank and a burdensome regime for the customers.

- A. Bank shall undertake identification of customers in the following cases:
- i. Commencement of an account-based relationship with the customer.
  - ii. Carrying out any international money transfer operations for a person who is not an account holder of the Bank.
  - iii. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
  - iv. Selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.
  - v. Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
  - vi. When a Bank has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
  - vii. Bank shall ensure that introduction is not to be sought while opening accounts.
- B. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, Bank, shall at their option, rely on customer due diligence done by a third party, subject to the following conditions:
- i. Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.
  - ii. Adequate steps are taken by Bank to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
  - iii. The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
  - iv. The third party shall not be based in a country or jurisdiction assessed as high risk.
  - v. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Bank.

### **13. Customer Due Diligence (CDD) Procedure**

#### **Customer Due Diligence (CDD) Procedure in case of Individuals**

For undertaking CDD, Bank shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

- A. The Aadhaar number where,
- i. he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or



- ii. he decides to submit his Aadhaar number voluntarily to a bank or any Bank notified under first proviso to sub-section (1) of section 11A of the PML Act; or
  - (a) the proof of possession of Aadhaar number where offline verification can be carried out; or
  - (b) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; or
  - (c) the KYC Identifier with an explicit consent to download records from CKYCR; and
- B. the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and
- C. one recent photograph
- D. such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the Bank.

Provided that where the customer has submitted,

- i. Aadhaar number under clause (a) above to a bank or to a BANK notified under first proviso to sub-section (1) of section 11A of the PML Act, such bank or BANK shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the Bank.
- ii. proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the BANK shall carry out offline verification.
- iii. an equivalent e-document of any OVD, the BANK shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under [Annex I](#).
- iv. any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the BANK shall carry out verification through digital KYC as specified under [Annex I](#).
- v. KYC Identifier under clause (ac) above, the BANK shall retrieve the KYC records online from the CKYCR in accordance with Section 56.

Provided that for a period not beyond such date as may be notified by the Government for a class of BANKs, instead of carrying out digital KYC, the BANK pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, BANKs shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other

OVD or the equivalent e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the Bank and such exception handling shall also be a part of the concurrent audit as mandated in Section 8. Bank shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the Bank and shall be available for supervisory review.

Explanation 1: Bank shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required as per proviso (i) above.

Explanation 2: Biometric based e-KYC authentication can be done by bank official/ business correspondents/business facilitators.

Explanation 3: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made there under.

#### SCHEDULE – 1

1. Primary Co-operative Credit Society which is being financed by the bank.
2. Khadi and Village Industries Boards.
3. Agriculture Produce Market Committees.
4. Societies registered under the Societies Registration Act, 1860 or any other corresponding law in force in a State or a Union Territory except societies registered under the State Co-operative Societies Acts and specific state enactment creating Land Mortgage Banks.
5. Companies licensed by the Central Government under Section 8 of Companies Act, 2013 or Section 25 of Companies Act, 1956 or under the corresponding provision in the Indian Companies Act, 1913 and permitted, not to add to their names the words 'Limited' or the words 'Private Limited'.
6. Institutions other than those mentioned in section 28(h) and whose entire income is exempt from payment of Income-tax under the Income-Tax Act, 1961.
7. Government departments / bodies / agencies in respect of grants/ subsidies released for implementation of various programmes / Schemes sponsored by Central Government / State Governments subject to production of an authorization from the respective Central / State Government departments to open savings bank account.
8. Development of Women and Children in Rural Areas (DWCRA).
9. Self-help Groups (SHGs), registered or unregistered, which are engaged in promoting savings habits among their members.
10. Farmers' Clubs – Vikas Volunteer Vahini – VVV.

#### **14. Accounts opened using OTP based e-KYC**

Accounts opened using Aadhaar OTP based e-KYC, in non-face-to-face mode, are subject to the following conditions:

- i. There must be a specific consent from the customer for authentication through OTP.

- ii. As a risk-mitigating measure for such accounts, Bank shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. Bank shall have a board approved policy delineating a robust process of due diligence for dealing with requests for change of mobile number in such accounts.
- iii. The aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (v) below is complete.
- iv. The aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.
- v. As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.
- vi. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Section 16 or as per Section 18 (V-CIP) is carried out. If Aadhaar details are used under Section 18, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.
- vii. If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits shall be allowed.
- viii. A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other Bank. Further, while uploading KYC information to CKYCR, Bank shall clearly indicate that such accounts are opened using OTP based e-KYC and other Bank shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.
- ix. Bank shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

## **15. V-CIP**

A. Bank may undertake V-CIP to carry out:

- i. CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.

Provided that in case of CDD of a proprietorship firm, Bank shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Section 28 and Section 29, apart from undertaking CDD of the proprietor.

- ii. Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per Section 17.

iii. Updation/Periodic updation of KYC for eligible customers.

B. Bank opting to undertake V-CIP, shall adhere to the following minimum standards:

**(a) V-CIP Infrastructure**

- i) The Bank should have complied with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises of the Bank and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines. Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the Bank only and all the data including video recording is transferred to the Bank exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the Bank.
- ii) The Bank shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.
- iii) The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.
- iv) The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.
- v) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Bank. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.
- vi) Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.
- vii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.
- viii) The V-CIP application software and relevant APIs / webservices shall also undergo appropriate testing of functional, performance, maintenance strength before being used in

live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

**(b) V-CIP Procedure**

- i) Each Bank shall formulate a clear work flow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the Bank specially trained for this purpose. The official should be capable to carry out liveness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.
- ii) Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the Bank. However, in case of call drop / disconnection, fresh session shall be initiated.
- iii) The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.
- iv) Any prompting observed at end of customer shall lead to rejection of the account opening process.
- v) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of work-flow.
- vi) The authorised official of the Bank performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:
  - a) OTP based Aadhaar e-KYC authentication
  - b) Offline Verification of Aadhaar for identification
  - c) KYC records downloaded from CKYCR, in accordance with Section 56, using the KYC identifier provided by the customer
  - d) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digi Locker

Bank shall ensure to redact or blackout the Aadhaar number in terms of Section 16.

In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than three working days from the date of carrying out V-CIP.

Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, Bank shall ensure that the video process of the V-CIP is undertaken within three working days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, Banks shall ensure that no incremental risk is added due to this.

- vii) If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.
- viii) Bank shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through Digi Locker.
- ix) Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.
- x) The authorised official of the Bank shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.
- xi) Assisted V-CIP shall be permissible when banks take help of Business Correspondents (BCs) facilitating the process only at the customer end. Banks shall maintain the details of the BC assisting the customer, where services of BCs are utilized. The ultimate responsibility for customer due diligence will be with the bank.
- xii) All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process and its acceptability of the outcome.
- xiii) All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the Bank.

**(c) V-CIP Records and Data Management**

- i) The entire data and recordings of V-CIP shall be stored in a system / systems located in India. Bank shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in this MD, shall also be applicable for V-CIP.
- ii) The activity log along with the credentials of the official performing the V-CIP shall be preserved.

**(d) Small Accounts**

Notwithstanding anything contained in Section 16 and as an alternative thereto, in case an individual who desires to open a bank account, bank shall open a 'Small Account', which entails the following limitations:

- i. the aggregate of all credits in a financial year does not exceed rupees one lakh;
- ii. the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and
- iii. the balance at any point of time does not exceed rupees fifty thousand.

Provided, that this limit on balance shall not be considered while making deposits through Government grants, welfare benefits and payment against procurements.

Further, small accounts are subject to the following conditions:

- i. The bank shall obtain a self-attested photograph from the customer.
- ii. The designated officer of the bank certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence

Provided that where the individual is a prisoner in a jail, the signature or thumb print shall be affixed in presence of the officer in-charge of the jail and the said officer shall certify the same under his signature and the account shall remain operational on annual submission of certificate of proof of address issued by the officer in-charge of the jail.

- iii. Such accounts are opened only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to the account.
- iv. Bank shall ensure that the stipulated monthly and annual limits on aggregate of transactions and balance requirements in such accounts are not breached, before a transaction is allowed to take place.
- v. The account shall remain operational initially for a period of twelve months which can be extended for a further period of twelve months, provided the account holder applies and furnishes evidence of having applied for any of the OVDs during the first twelve months of the opening of the said account.
- vi. The entire relaxation provisions shall be reviewed after twenty four months.
- vii. Notwithstanding anything contained in clauses (e) and (f) above, the small account shall remain operational between April 1, 2020 and June 30, 2020 and such other periods as may be notified by the Central Government.
- viii. The account shall be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high risk scenarios, the identity of the customer shall be established as per Section 16 or Section 18.
- ix. Foreign remittance shall not be allowed to be credited into the account unless the identity of the customer is fully established as per Section 16 or Section 18.

## **16. KYC verification**

KYC verification once done by one branch/office of the bank shall be valid for transfer of the account to any other branch/office of the same bank, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

## **17. Customer Due Diligence (CDD) Measures for Sole Proprietary firms**

- A.i. For opening an account in the name of a sole proprietary firm, CDD in respect of the individual (proprietor) shall be carried out.
- ii. Keeping in view the importance of credit discipline for reduction in Non Performing Assets (NPA) level of bank, bank should insist on a declaration from the account-holder to the effect that he is not enjoying any credit facility with any other bank or obtain a declaration giving particulars of credit facilities enjoyed by him with any other bank(s). The account opening bank should ascertain all the details and should also inform the concerned lending bank(s). The account-opening bank should obtain No objection Certificate from such banks.

iii. However, in case no response is received from the existing bankers after a minimum period of a fortnight, banks may open current accounts of prospective customers.

iv. Further, where the due diligence is carried out on the request of a prospective customer who is a corporate customer or a large borrower enjoying credit facilities from more than one bank, the bank may inform the consortium leader, if under consortium, and the concerned banks, if under multiple banking arrangement.

B. In addition to the above, any two of the following documents as a proof of business/ activity in the name of the **proprietary firm** shall also be obtained :

- i. Registration certificate including Udhyam Registration Certificate (URD) issued by Govt.
- ii. Certificate/licence issued by the municipal authorities under Shop and Establishment Act.
- iii. Sales and income tax returns.
- iv. CST/VAT/ GST certificate (provisional/final).
- v. Certificate/registration document issued by Sales Tax/Service Tax/ Professional Tax authorities.
- vi. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT/Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
- vii. Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/ acknowledged by the Income Tax authorities.
- viii. Utility bills such as electricity, water, and landline telephone bills.
- ix. Copy of Aadhar Card and PAN Card of the proprietor.
- x. Photographs of the Proprietor.

C. In cases where the bank is satisfied that it is not possible to furnish two such documents, bank may, at their discretion, accept only one of those documents as proof of business/activity.

Provided bank undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

## 18. CDD Measures for Legal Entities

A. For opening an **account of a company**, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained :

- i. Certificate of incorporation
- ii. Memorandum and Articles of Association
- iii. Permanent Account Number of the company
- iv. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
- v. Keeping in view the importance of credit discipline for reduction in Non Performing Assets (NPA) level of bank, bank should insist on a declaration from the account-holder to the effect that he is not enjoying any credit facility with any other bank or obtain a



declaration giving particulars of credit facilities enjoyed by him with any other bank(s). The account opening bank should ascertain all the details and should also inform the concerned lending bank(s). The account-opening bank should obtain No objection Certificate from such banks.

- vi. However, in case no response is received from the existing bankers after a minimum period of a fortnight, banks may open current accounts of prospective customers.
  - vii. Further, where the due diligence is carried out on the request of a prospective customer who is a corporate customer or a large borrower enjoying credit facilities from more than one bank, the bank may inform the consortium leader, if under consortium, and the concerned banks, if under multiple banking arrangement.
  - viii. Documents, as specified in Section 16, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf
  - ix. the names of the relevant persons holding senior management position; and
  - x. the registered office and the principal place of its business, if it is different
  - xi. Copy of Aadar Card and PAN Card of the Directors authorized to operate the account.
  - xii. Photographs of the Directors authorized to operate the account.
- B. For opening an **account of a partnership firm**, the certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
- i. Registration certificate
  - ii. Partnership deed
  - iii. Permanent Account Number of the partnership firm
  - iv. Copy of Aadar Card and PAN Card of the partner authorized to operate the account.
  - v. Photographs of the partner authorized to operate the account.
  - vi. Keeping in view the importance of credit discipline for reduction in Non Performing Assets (NPA) level of banks, banks should insist on a declaration from the account-holder to the effect that he is not enjoying any credit facility with any other bank or obtain a declaration giving particulars of credit facilities enjoyed by him with any other bank(s). The account opening bank should ascertain all the details and should also inform the concerned lending bank(s). The account-opening bank should obtain No objection Certificate from such banks.
  - vii. However, in case no response is received from the existing bankers after a minimum period of a fortnight, banks may open current accounts of prospective customers.
  - viii. Further, where the due diligence is carried out on the request of a prospective customer who is a corporate customer or a large borrower enjoying credit facilities from more than one bank, the bank may inform the consortium leader, if under consortium, and the concerned banks, if under multiple banking arrangement.
  - ix. Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
  - x. the names of all the partners and
  - xi. address of the registered office, and the principal place of its business, if it is different.
- C. For opening an **account of a trust**, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained :
- i. Registration certificate
  - ii. Trust deed
  - ii. Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf

- iii. the names of the beneficiaries, trustees, settlor and authors of the trust
  - iv. address of the registered office of the trust; and the
  - v. list of trustees and documents, as specified in Section 16, for those discharging the role as trustee and authorised to transact on behalf of the trust.
  - vi. Permanent Account Number or Form No.60 of the trust
  - vii. Keeping in view the importance of credit discipline for reduction in Non Performing Assets (NPA) level of banks, banks should insist on a declaration from the account-holder to the effect that he is not enjoying any credit facility with any other bank or obtain a declaration giving particulars of credit facilities enjoyed by him with any other bank(s). The account opening bank should ascertain all the details and should also inform the concerned lending bank(s). The account-opening bank should obtain No objection Certificate from such banks.
  - viii. However, in case no response is received from the existing bankers after a minimum period of a fortnight, banks may open current accounts of prospective customers.
  - ix. Further, where the due diligence is carried out on the request of a prospective customer who is a corporate customer or a large borrower enjoying credit facilities from more than one bank, the bank may inform the consortium leader, if under consortium, and the concerned banks, if under multiple banking arrangement.
  - x. Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
  - xi. Copy of Aadar Card and PAN Card of the Trustees authorized to operate the account.
  - xii. Photographs of the Trustees authorized to operate the account.
- D. For opening an account of an **unincorporated association** or **a body of individuals**, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained :
- i. Resolution of the managing body of such association or body of individuals
  - ii. Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals
  - iii. Power of attorney granted to transact on its behalf
  - iv. relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and Documents, as specified in Section 16,
  - v. Such information as may be required by the bank to collectively establish the legal existence of such an association or body of individuals.
  - vi. Keeping in view the importance of credit discipline for reduction in Non Performing Assets (NPA) level of banks, banks should insist on a declaration from the account-holder to the effect that he is not enjoying any credit facility with any other bank or obtain a declaration giving particulars of credit facilities enjoyed by him with any other bank(s). The account opening bank should ascertain all the details and should also inform the concerned lending bank(s). The account-opening bank should obtain No objection Certificate from such banks.
  - vii. However, in case no response is received from the existing bankers after a minimum period of a fortnight, banks may open current accounts of prospective customers.
  - viii. Further, where the due diligence is carried out on the request of a prospective customer who is a corporate customer or a large borrower enjoying credit facilities from more than one bank, the bank may inform the consortium leader, if under consortium, and the concerned banks, if under multiple banking arrangement.
  - ix. Copy of Aadar Card and PAN Card of the associated/individual persons authorised to operate the account.

- x. Photographs of the associated/individual persons authorised to operate the account.

Explanation : Unregistered trusts/partnership firms shall be included under the term 'unincorporated association'.

Explanation : Term 'body of individuals' includes societies.

## 19. Identification of Beneficial Owner

For opening an **account of a Legal Person** who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps in terms of sub-rule (3) of Rule 9 of the Rules to verify his/her identity shall be undertaken keeping in view the following:

- i. Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.
- ii. In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

## 20. On-going Due Diligence

Bank shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.

Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:

- i. Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
- ii. Transactions which exceed the thresholds prescribed for specific categories of accounts.
- iii. High account turnover inconsistent with the size of the balance maintained.
- iv. Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

For ongoing due diligence, Bank may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring.

## 21. Extent of Monitoring

The extent of monitoring shall be aligned with the risk category of the customer.

Explanation: High risk accounts have to be subjected to more intensified monitoring.

- i) A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

- ii) The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored.

Explanation: Cases where a large number of cheque books are sought by the company and/or multiple small deposits (generally in cash) across the country in one bank account and/or where a large number of cheques are issued bearing similar amounts/dates, shall be immediately reported to Reserve Bank of India and other appropriate authorities such as FIU-IND.

## **22 Monitoring Operations**

### **A. Monitoring Operations in New Accounts**

- i. It shall be the responsibility of the Branch In-charge/Managers to maintain a close watch over the operations in newly opened accounts at least for the first six months, from the date of opening of such accounts, keep a close watch, so as to guard against fraudulent or doubtful transactions taking place therein. If any transaction of suspicious nature is revealed, branch should enquire about the transaction from the account holder, and if no convincing explanation is forthcoming, they should consider reporting such transactions to the appropriate investigating agencies.
- ii. 21.1.2 Caution should be exercised whenever cheques/ drafts for large amounts are presented for collection, or Telegraphic Transfers (TTs)/Mail Transfers (MTs) are received for credit of new accounts immediately/within a short period after opening of account. In such cases, genuineness of the instruments and the account holder should be thoroughly verified. If necessary the paying bank should check with the collecting bank about the genuineness of any large value cheques/drafts issued. Demand Drafts (DDs)/Cheques for large amounts presented for collection should be verified under ultra violet lamps to safe guard against chemical alterations.

### **B. Monitoring Operations in all Accounts**

- i. It shall be the responsibility of the Branch In-charge/Managers to maintain a close monitoring of cash withdrawal for large amounts. Where third party cheques, drafts, etc. are deposited in the existing and newly opened accounts followed by cash withdrawals for large amounts, the banks should keep a proper vigil over the requests of their clients for such cash withdrawals for large amounts.
- ii. The bank should closely monitoring cash deposits and withdrawals for Rs. 5 lakh and above not only in deposit accounts but also in all other accounts like cash credit/overdraft etc. The bank/branches should also maintain a separate register to record details of individual cash deposits and withdrawals for Rs. 5 lakh and above. The details recorded should include, in the case of deposits, the name of the account holder, account number, amount deposited and in the case of withdrawals, the name of the account holder, account number, amount of withdrawal and name of the beneficiary of the cheque. Further, any cash deposits or withdrawals of Rs. 5 lakh and above should be reported by the Branch Manager to the Head Office on a fortnightly basis along with full particulars, such as name of the account holder, account number, date of opening the account, etc. On receipt of these statements from branches, the Head Office should immediately scrutinise the details thereof and have the transactions looked into by deputing officials, if the transactions prima facie appear to be dubious or giving rise to suspicion. The inspecting officials from the Reserve Bank during the course of their inspections will also be looking into the statements submitted by the branches.
- iii. The other important areas in the payment of cheques wherein due caution need to be exercised are verification of drawer's signature, custody of specimen signature cards, supervision over issue of cheque books and control over custody of blank cheque books/leaves. While need for

examining cheques for large amounts under Ultra Violet Ray Lamps is recognised by the branches, in practice it is rarely done as there is often a tendency to be lax in the matter resulting in avoidable loss. In addition, due care should be exercised in regard to issue and custody of tokens, movement of cheques tendered across the counter and custody of all instruments after they are paid by the banks. Depositors/ Customers should be asked to surrender unused cheque books before closing/transferring the accounts. Also safe custody of specimen signature cards is of utmost importance, especially when operating instructions are changed, the change should be duly verified by a senior official in the branch.

### C. Issue of Cheque Books

Fresh cheque books should be issued only against production of duly signed requisition slips from previous cheque book issued to the party. In case the cheque book is issued against a requisition letter, the drawer should be asked to come personally to the bank or cheque book should be sent to him under registered post directly without being delivered to the bearer. Loose cheques should be issued to account holder only when they come personally with a requisition letter and on production of passbooks.

## 23. Periodic Updation of KYC

A. Bank shall adopt a risk-based approach for periodic updation of KYC. However, periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers from the date of opening of the account / last KYC updation. Policy in this regard shall be documented as part of Bank internal KYC policy duly approved by the Board of Directors of Bank or any committee of the Board to which power has been delegated.

### i. Individual Customers:

- a) **No change in KYC information:** In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the Bank, customer's mobile number registered with the Bank, ATMs, digital channels (such as online banking / internet banking, mobile application of Bank), letter etc.
- b) **Change in address:** In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the Bank, customer's mobile number registered with the Bank, ATMs, digital channels (such as online banking / internet banking, mobile application of Bank), letter etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc. Further, Bank, at their option, may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as defined in Section 3(a)(xiii), for the purpose of proof of address, declared by the customer at the time of periodic updation. Such requirement, however, shall be clearly specified by the Bank in their internal KYC policy duly approved by the Board of Directors of Bank or any committee of the Board to which power has been delegated.
- c) **Accounts of customers, who were minor at the time of opening account, on their becoming major :**
  - (i) In case of customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD documents as per the current CDD standards are available with the

Bank. Wherever required, REs may carry out fresh KYC of such customers i.e. customers for whom account was opened when they were minor, on their becoming a major.

(ii) Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation. To clarify, conditions stipulated in Section 17 are not applicable in case of updation / periodic updation of KYC through Aadhaar OTP based e-KYC in non-face to face mode.

(iii) declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. REs shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud

**d) Customers other than individuals:**

(i) No change in KYC information: In case of no change in the KYC information of the LE customer, a self-declaration in this regard shall be obtained from the Legal Entity customer through its email id registered with the RE, ATMs, digital channels (such as online banking / internet banking, mobile application of Bank), letter from an official authorized by the LE in this regard, board resolution etc. Further, Bank shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-to date as possible.

(ii) **Change in KYC information:** In case of change in KYC information, Bank shall undertake the KYC process equivalent to that applicable for on boarding a new Legal Entity customer.

**e) Additional measures: In addition to the above, Bank shall ensure that,**

(i) The KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available with the Bank are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the RE has expired at the time of periodic updation of KYC, Bank shall undertake the KYC process equivalent to that applicable for on-boarding a new customer

(ii) Customer's PAN details, if available with the Bank is verified from the database of the issuing authority at the time of periodic updation of KYC.

(iii) Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the Bank and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

(iv) In order to ensure customer convenience, Bank may consider making available the facility of periodic updation of KYC at any branch, in terms of their internal KYC policy duly approved by the Board of Directors of Bank or any committee of the Board to which power has been delegated.

(v) Bank shall adopt a risk-based approach with respect to periodic updation of KYC. Any additional and exceptional measures, which otherwise are not mandated under the above instructions, adopted by the Bank such as requirement of obtaining recent photograph,

requirement of physical presence of the customer, requirement of periodic updation of KYC only in the branch of the Bank where account is maintained, a more frequent periodicity of KYC updation than the minimum specified periodicity etc., shall be clearly specified in the internal KYC policy duly approved by the Board of Directors of Bank or any committee of the Board to which power has been delegated.

- (vi) Bank shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the REs the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at Bank's end.

## **24. Existing Customers,**

In case of existing customers, Bank shall obtain the Permanent Account Number or equivalent e-document thereof or Form No.60, by such date as may be notified by the Central Government, failing which Bank shall temporarily cease operations in the account till the time the Permanent Account Number or equivalent e-documents thereof or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, the Bank shall give the customer an accessible notice and a reasonable opportunity to be heard.

Further, Bank shall include, in its internal policy, appropriate relaxation(s) for continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes. Such accounts shall, however, be subject to enhanced monitoring.

Provided further that if a customer having an existing account-based relationship with a Bank gives in writing to the Bank that he does not want to submit his Permanent Account Number or equivalent e-document thereof or Form No.60, Bank shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

Explanation - For the purpose of this Section, "temporary ceasing of operations" in relation an account shall mean the temporary suspension of all transactions or activities in relation to that account by the Bank till such time the customer complies with the provisions of this Section. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.

## **25. Enhanced and Simplified Due Diligence Procedure**

### **A. Enhanced Due Diligence**

- i.a) In case Bank has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP for the purpose of this Master Direction.
- b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from

the mobile number used for account opening. RE shall have a Board approved policy delineating a robust process of due diligence for dealing with requests for change of registered mobile number.

- c) Apart from obtaining the current address proof, Bank shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.
- d) Bank shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
- e) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.
- f) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP. Accounts of Politically Exposed Persons (PEPs)

## **ii. Accounts of Politically Exposed Persons (PEPs)**

- a) bank shall have the option of establishing a relationship with PEPs provided that:
  - (a) sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
  - (b) the identity of the person shall have been verified before accepting the PEP as a customer;
  - (c) the decision to open an account for a PEP is taken at a senior level in accordance with the bank's Customer Acceptance Policy;
  - (d) all such accounts are subjected to enhanced monitoring on an on-going basis;
  - (e) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;
  - (f) the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.
- b) These instructions shall also be applicable to accounts where a PEP is the beneficial owner.

## **iii. Client accounts opened by professional intermediaries:**

Bank shall ensure while opening client accounts through professional intermediaries, that:

- a) Clients shall be identified when client account is opened by a professional intermediary on behalf of a single client.
- b) bank shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
- c) bank shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the bank.



- d) all the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of bank, and there are 'sub-accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of bank, the bank shall look for the beneficial owners.
- e) bank shall, at their discretion, rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.
- f) The ultimate responsibility for knowing the customer lies with the bank.

## **B. Simplified Due Diligence**

### **i. Norms for Self Help Groups (SHGs) Simplified**

- a) CDD of all the members of SHG as per the CDD procedure mentioned in Section 15 of the MD shall not be required while opening the savings bank account of the SHG
- b) CDD as per the CDD procedure mentioned in Section 15 of the MD of all the office bearers shall suffice.
- c) No separate CDD as per the CDD procedure mentioned in Section 15 of the MD of the members or office bearers shall be necessary at the time of credit linking of SHGs

### **ii. Opening accounts of foreign students**

Banks shall not open a Non Resident Ordinary (NRO) bank account of a foreign student.

### **iii. Simplified KYC norms for Foreign Portfolio Investors (FPIs)**

Bank shall not open Foreign Portfolio Investors (FPIs) accounts.

## **26. Record Management**

- A. The following steps shall be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules. banks shall,
  - i. maintain all necessary records of transactions between the bank and the customer, both domestic and international, for at least five years from the date of transaction;
  - ii. preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;
  - iii. make available the identification records and transaction data to the competent authorities upon request;
  - iv. introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
  - v. maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:

- a) the nature of the transactions;
  - b) the amount of the transaction and the currency in which it was denominated;
  - c) the date on which the transaction was conducted; and
  - d) the parties to the transaction.
- vi. evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;
  - vii. maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

Explanation. – For the purpose of this Section, the expressions "records pertaining to the identification", "identification records", etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.

- B. Bank shall ensure that in case of customers who are non-profit organisations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, Bank shall register the details on the DARPAN Portal. Bank shall also maintain such registration records for a period of five years after the business relationship between the customer and the Bank has ended or the account has been closed, whichever is later.

## **27. Reporting Requirements to Financial Intelligence Unit - India**

- A. i. Bank shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.

Explanation: In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND shall have powers to issue guidelines to the Bank for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.

- ii. The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by Bank which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data.
- iii. While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. Bank shall not put any restriction on operations in the accounts where an STR has been filed. Bank shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.
- iv. Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

## **B. Procedure and manner of furnishing information.**

- i. Bank shall communicate to the Director FIU-IND, the name, designation and address of the Designated Director and the Principal Officer.
- ii. The Principal Officer shall furnish the information referred to in clauses (A), (B), (BA), (C), (D), (E) and (F) of sub-rule (1) of rule 3 to the Director on the basis of information available with the reporting entity. A copy of such information shall be retained by the Principal Officer for the purposes of official record.
- iii. Bank shall evolve an internal mechanism having regard to any guidelines issued by regulator, for detecting the transactions referred to in clauses (A), (B), (BA), (C), (D), (E) and (F) of sub-rule (1) of rule 3 and for furnishing information about such transactions in such form as may be directed by its Regulator.
- iv. It shall be the duty of bank, its designated director, officers and employees to observe the procedure and the manner of furnishing information as specified by Regulatory Authorities.

## **C. Furnishing of information to the Director.—**

- i. The Principal Officer of the bank shall furnish the information in respect of transactions referred to in clauses (A), (B), (BA), (C) and (E) of sub-rule (1) of rule 3 every month to the Director by the 15th day of the succeeding month.
- ii. The Principal Officer of the bank shall furnish the information promptly in writing or by fax or by electronic mail to the Director in respect of transactions referred to in clause (D) of sub-rule (1) of rule 3 not later than seven working days on being satisfied that the transaction is suspicious.
- iii. The Principal Officer of the bank shall furnish, the information in respect of transactions referred to in clause (F) of sub-rule (1) of rule 3, every quarter to the Director by the 15th day of the month succeeding the quarter.
- iv. For the purpose of this rule, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-reported transaction beyond the time limit as specified in this rule shall constitute a separate violation.

## **D. Overview of Reporting under PMLA**

- i. All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;
- ii. All series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month;
- iii. All transactions involving receipts by non-profit organisations of value more than rupees ten lakh, or its equivalent in foreign currency.
- iv. All cash transactions where forged or counterfeit currency notes or banknotes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions.
- v. All suspicious transactions whether or not made in cash.
- vi. All cross- border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India.

- vii. All purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity, as the case may be.
- viii. The bank is required to furnish to FIU-IND following information under Prevention of Money Laundering Act, 2002 and the Rules there under.

#### **E. Cash Transaction Reports**

The Prevention of Money-laundering Act, 2002, and rule there under require every reporting entity to furnish to FIU-IND information relating to -

- i. All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;

All series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency.

#### **F. Counterfeit Currency Reports**

The Prevention of Money-laundering Act, 2002, and rule thereunder require every banking company, financial institution and intermediary, to furnish to FIU-IND information relating to all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions.

#### **G. Wire Transfer**

Bank shall ensure the following while effecting wire transfer:

- i. All cross-border wire transfers including transactions using credit or debit card shall be accompanied by accurate and meaningful originator information such as name, address and account number or a unique reference number, as prevalent in the country concerned in the absence of account. Exception: Interbank transfers and settlements where both the originator and beneficiary are banks or financial institutions shall be exempt from the above requirements.
- ii. Domestic wire transfers of rupees fifty thousand and above shall be accompanied by originator information such as name, address and account number.
- iii. Customer Identification shall be made if a customer is intentionally structuring wire transfer below rupees fifty thousand to avoid reporting or monitoring. In case of non-cooperation from the customer, efforts shall be made to establish his identity and STR shall be made to FIU-IND.
- iv. Complete originator information relating to qualifying wire transfers shall be preserved at least for a period of five years by the ordering bank.
- v. A bank processing as an intermediary element of a chain of wire transfers shall ensure that all originator information accompanying a wire transfer is retained with the transfer.
- vi. The receiving intermediary bank shall transfer full originator information accompanying a cross-border wire transfer and preserve the same for at least five years if the same cannot be sent with a related domestic wire transfer, due to technical limitations.
- vii. All the information on the originator of wire transfers shall be immediately made available to appropriate law enforcement and/or prosecutorial authorities on receiving such requests.

- viii. Effective risk-based procedures to identify wire transfers lacking complete originator information shall be in place at a beneficiary bank.
- ix. Beneficiary bank shall report transaction lacking complete originator information to FIU-IND as a suspicious transaction.
- x. The beneficiary bank shall seek detailed information of the fund remitter with the ordering bank and if the ordering bank fails to furnish information on the 44 remitter, the beneficiary shall consider restricting or terminating its business relationship with the ordering bank.

#### **H. Report on sale/purchase of immovable property**

Bank is required to furnish to Director, FIU-IND the report on all purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity as the case may be.

#### **I. Suspicious Transaction Reports**

Bank shall furnish to FIU-IND information of all suspicious transactions whether or not made in cash.

Suspicious transaction means a transaction referred to in clause (h) of the rules, including an attempted transaction, whether or not made in cash which, to a person acting in good faith –

- i. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
- ii. appears to be made in circumstances of unusual or unjustified complexity; or
- iii. appears to have no economic rationale or bonafide purpose; or
- iv. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;
- v. Locker Operations  
Accounts linked to the lockers wherein frequent operations are observed shall be analysed as sometimes instances are noticed like, cash is withdrawn and immediately the lockers is operated or locker is operated followed by deposit in cash. These activities aroused suspicious and hence be reported.

#### **J. Cash Transactions Report [CTR]**

- i. Report of all cash transactions of the value of more than rupee ten lakhs or its equivalent in foreign currency and all series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transaction exceeds Rupees ten lakh.
- ii. The CTR for each month will be submitted to FIU-IND by 15th of the succeeding month.
- iii. A copy of monthly CTR submitted on its behalf to FIU-IND is available at the concerned branch (through MIS Report: Misc Reports Module under SENSRPT – 5/7 & 5/7a) for production to auditors/Inspectors, when asked for. While determining suspicious transactions, bank is to be guided by the definition of “suspicious transaction” as contained in PMLA Rules as amended from time to time.

## K. Suspicious Transaction Reports (STR)

- i. While determining suspicious transactions, bank is to be guided by the definition of “suspicious transaction” as contained in PMLA Rules as amended from time to time.

**"Suspicious transaction"** means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

- (a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
- (b) appears to be made in circumstances of unusual or unjustified complexity ;or
- (c) appears to not have economic rationale or bona-fide purpose; or
- (d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

- ii. It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. All such attempted transactions in STRs to be reported, even if not completed by the customers, irrespective of the amount of the transaction.
- iii. STR to be submitted if it has reasonable ground to believe that the transaction involves proceeds of crime irrespective of the amount of the transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.
- iv. Furnishing of STR to be ensured within seven days of arriving at a conclusion by the Principal Officer of the Bank that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature.
- v. It shall be ensured not to put any restrictions on operations in the accounts where an STR has been filed. The submission of STR will be kept strictly confidential, as required under PML Rules and it will be ensured that there is no tipping off to the customer at any level.
- vi. The primary responsibility for monitoring and reporting of suspicious transaction shall be of the branch. The monitoring of the transactions will also be done by controlling offices, who will also interact with the branches to facilitate monitoring and reporting of suspicious transactions. Controlling offices shall monitor transactions in customer accounts, in general, and high risk accounts/ high value transactions, in particular.
- vii. For effective monitoring of transactions of the customers, Bank has implemented an AML system for generation of AML alerts on day to day basis based on the pre-defined scenarios, as advised by Indian Banks Association (IBA) / Financial Intelligence Unit – India (FIU-IND) from time to time. These scenarios will be periodically reviewed to make them more effective based on the feedback received and experience gained. Further, an indicative list of behavioral /observation based scenarios has been circulated vide Centralised AML Cell (FRMD) Circular No. 01/2021 dated 22.01.2021. In case any suspicious transaction is detected, the same be reported to Centralised AML Cell for onward submission of Suspicious Transaction Report (STR) to Financial Intelligence Unit – India (FIU-IND) through FIN net Gateway after getting the approval of Principal Officer of the Bank.

Indicative list of various types of indicators i.e. customer behavior and risk based transaction monitoring (RBTM), high & medium risk: customers/products & services/ geographies/ locations/alerts for branches/departments, are attached at **Annexure-III** of Operational Guidelines for KYC Policy for FY 2023-2024.

#### **L. Counterfeit Currency Report (CCR)**

Cash transactions were forged or counterfeit currency notes have been used as genuine or where any forgery of a valuable security or document has taken place facilitating the transactions will be reported to Financial Intelligence Unit-India in the specified format by 15th of the succeeding month.

#### **M. Non Profit Organisations Transaction report [NTR]**

All transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency, to be reported to the Director, Financial Intelligence Unit-India by the 15th of the succeeding month.

#### **N. Cross-border Wire Transfer Report [CWTR]**

Cross-Border Wire Transfer Report (CWTR) to be filed to the Director, Financial Intelligence Unit-India by 15th of succeeding month for all cross border wire transfers of the value of more than Rs 5 lakh or its equivalent in foreign currency where either the origin or destination of fund is in India.

#### **N. Identity of client**

- a) False identification documents
- b) Identification documents which could not be verified within reasonable time
- c) Accounts opened with names very close to other established business entities

#### **O. Background of client**

Suspicious background or links with known criminals

#### **P. Multiple accounts**

- a) Large number of accounts having a common account holder, introducer or authorized signatory with no rationale
- b) Unexplained transfers between multiple accounts with no rationale

#### **Q. Activity in accounts**

- D. Unusual activity compared with past transactions
- E. Sudden activity in dormant accounts
- F. Activity inconsistent with what would be expected from declared business

#### **R. Nature of transactions**

- a) Unusual or unjustified complexity
- b) No economic rationale or bonafide purpose
- c) Frequent purchases of drafts or other negotiable instruments with cash
- d) Nature of transactions inconsistent with what would be expected from declared business

#### **S. Value of transactions**

- a) Value just under the reporting threshold amount in an apparent attempt to avoid reporting
- b) Value inconsistent with the client's apparent financial standing

Broad categories of reason for suspicion and examples of suspicious transactions for an

intermediary are indicated as under :

### Reports & their periodicity

#### Due Dates for filing Reports

Report	Description	Due Date
CTR	All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency.	15 <sup>th</sup> day of the succeeding month
	All series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month	
CCR	All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions	
NTR	All transactions involving receipts by non profit organizations of value more than Rs. Ten lakhs or, its equivalent in foreign currency	
CBWTR	All cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India.	
IPR	All purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity, as the case may be.	
STR	All suspicious transactions whether or not made in cash	Not later than seven working days on being satisfied that the transaction is suspicious.

T. Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

U. Alerts for identification of suspicious transactions. (Annexure – II)

#### 28. Requirements/obligations under International Agreements -

##### Communications from International Agencies

##### A. Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967:

- i. Bank shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, they do not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under:



a) **The “ISIL (Da’esh) & Al-Qaida Sanctions List”**, established and maintained pursuant to Security Council resolutions 1267/1989/2253, which includes names of individuals and entities associated with the Al-Qaida is available at <https://scsanctions.un.org/ohz5jen-al-qaida.html>

b) **The “Taliban Sanctions List”**, established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at <https://scsanctions.un.org/3pppl1en-taliban.htm>

Bank shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, shall be verified on daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the Bank for meticulous compliance.

ii . Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs (MHA) as required under UAPA notification dated February 2, 2021 (Annex II of this Master Direction).

iii. Freezing of Assets under Section 51A of UAPA, 1967: The procedure laid down in the UAPA Order dated 106February 2, 2021 (Annex II of this Master Direction) shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of MHA.

## **29. Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):**

i. Bank shall ensure meticulous compliance with the “Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005” laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated January 30, 2023, by the Ministry of Finance, Government of India (Annex III of this Master Direction).

ii. In accordance with paragraph 3 of the aforementioned Order, Bank shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

iii. Further, Bank shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.

iv. In case of match in the above cases, Bank shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. REs shall file an STR with FIU-IND covering all transactions in the accounts, covered above, carried through or attempted.

It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.

v. Bank shall refer to the designated list, as amended from time to time, available on the portal of FIU-India.

- vi. In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A of the WMD Act, 2005, Bank shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.
  - vii. In case an order to freeze assets under Section 12A is received by the Bank from the CNO, Bank shall, without delay, take necessary action to comply with the Order.
  - viii. The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by Bank along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.
30. Bank shall verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available at <https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm>, to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the 'Implementation of Security Council Resolution on Democratic People's Republic of Korea Order, 2017', as amended from time to time by the Central Government.
- 30A. In addition to the above, Bank shall take into account – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of Section 51A of the UAPA and Section 12A of the WMD Act.

### **31. Jurisdictions that do not or insufficiently apply the FATF Recommendations**

- i. FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account.
  - ii. Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.  
  
Explanation: The processes referred to in (a) & (b) above do not preclude REs from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.
  - iii. The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all documents shall be retained and shall be made available to Reserve Bank/other relevant authorities, on request.
- 31A. Bank shall encouraged to leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.104Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967:

## Other Instructions

### 32. Secrecy Obligations and Sharing of Information :

- i. Banks shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer.
- ii. Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.
- iii. While considering the requests for data/information from Government and other agencies, banks shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the banking transactions.
- iv. The exceptions to the said rule shall be as under:
  - a) Where disclosure is under compulsion of law
  - b) Where there is a duty to the public to disclose,
  - c) the interest of bank requires disclosure and
  - d) Where the disclosure is made with the express or implied consent of the customer.

### 33. CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)

- i. Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No.
- ii. S.O. 3183(E) dated November 26, 2015.
- iii. In terms of provision of Rule 9(1A) of PML Rules, the Bank shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.
- iv. Operational Guidelines for uploading the KYC data have been released by CERSAI.
- v. Bank shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.
- vi. The 'live run' of the CKYCR started from July 15, 2016 in phased manner beginning with new 'individual accounts'. Accordingly, Scheduled Commercial Banks (SCBs) are required to invariably upload the KYC data pertaining to all new individual accounts opened on or after January 1, 2017, with CKYCR. 39 SCBs were initially allowed time up-to February 1, 2017, for uploading data in respect of accounts opened during January 2017. Bank other than SCBs were required to start uploading the KYC data pertaining to all new individual accounts opened on or after from April 1, 2017, with CKYCR in terms of the provisions of the Rules *ibid*.
- vii. Bank shall upload KYC records pertaining to accounts of Legal Entities opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules *ibid*. The KYC records have to be uploaded as per the Legal Entities Template released by CERSAI.

- viii. Once KYC Identifier is generated by CKYCR, Bank shall ensure that the same is communicated to the individual/LE as the case may be.
- ix. In order to ensure that all KYC records are incrementally uploaded on to CKYCR, Bank shall upload/update the KYC data pertaining to accounts of individual customers and Legal Entities opened prior to the above mentioned dates as per (E) and (F) respectively at the time of periodic updation as specified in Section 38 of this Master Direction, or earlier, when the updated KYC information is obtained/received from the customer.
- x. Bank shall ensure that during periodic updation, the customers are migrated to the current CDD standard.
- xi. Where a customer, for the purposes of establishing an account based relationship, submits a KYC Identifier to a Bank with an explicit consent to download records from CKYCR, then such Bank shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless –
- a) there is a change in the information of the customer as existing in the records of CKYCR;
  - b) the current address of the customer is required to be verified;
  - c) the Bank considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

#### **34. Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)**

- i. Under FATCA and CRS, bank shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements :
- ii. Register on the related e-filing portal of Income Tax Department as Reporting Financial Institutions at the link <https://incometaxindiaefiling.gov.in/> post login --> My Account --> Register as Reporting Financial Institution,
- iii. Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to.  
Explanation: bank shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at <http://www.fedai.org.in/RevaluationRates.aspx> for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H.
- iv. Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H.
- v. Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.

- vi. Constitute a “High Level Monitoring Committee” under the Designated Director or any other equivalent functionary to ensure compliance.
- vii. Ensure compliance with updated instructions/ rules/ guidance notes/ Press releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to time and available on the web site <http://www.incometaxindia.gov.in/Pages/default.aspx>. Banks may take note of the following:
  - a) updated Guidance Note on FATCA and CRS
  - b) a press release on ‘Closure of Financial Accounts’ under Rule 114H (8).

### **35. Period for presenting payment instruments**

Payment of cheques/drafts/pay orders/banker’s cheques, if they are presented beyond the period of three months from the date of such instruments, shall not be made.

### **36. Operation of Bank Accounts & Money Mules**

The instructions on opening of accounts and monitoring of transactions shall be strictly adhered to, in order to minimise the operations of “Money Mules” which are used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties which act as “money mules.” If it is established that an account opened and operated is that of a Money Mule, it shall be deemed that the bank has not complied with these directions.

### **37. Collection of Account Payee Cheques**

Account payee cheques for any person other than the payee constituent shall not be collected. Banks shall, at their option, collect account payee cheques drawn for an amount not exceeding rupees fifty thousand to the account of their customers who are co-operative credit societies, provided the payees of such cheques are the constituents of such co-operative credit societies.

### **38. Unique Customer Identification Code (UCIC)**

A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers as also the existing customers by bank.

The bank shall, at their option, not issue UCIC to all walk-in/occasional customers such as buyers of pre-paid instruments/purchasers of third party products provided it is ensured that there is adequate mechanism to identify such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

### **39. Introduction of New Technologies – Credit Cards/Debit Cards/ Smart Cards/Gift Cards/Mobile Wallet/Net Banking/Mobile Banking/RTGS/NEFT/ ECS/ IMPS etc.**

Adequate attention shall be paid by bank to any money-laundering and financing of terrorism threats that may arise from new or developing technologies and it shall be ensured that appropriate KYC procedures issued from time to time are duly applied before introducing new products/services/technologies. Agents used for marketing of credit cards shall also be subjected to due diligence and KYC measures.

#### **40. Correspondent Banking**

The Bank i.e. the Janata Co-operative Bank Ltd. is having Real Time Gross Settlement(RTGS), National Electronic Fund Transfer(NEFT), Automated Teller Machine(ATM), National Automated Clearing House(NACH), Immediate Payment System (IMPS), Point of Sale (POS), Unified Payment Interface (UPI), issue of cheque at par facility, Constituent Subsidiary General Ledger(CSGL) etc. arrangements with HDFC Bank Ltd. and NPCI for which the necessary approval of the Board of Directors has been obtained prior to making these such arrangements and agreements to this effect have also signed by both the parties.

#### **41. Wire Transfer**

The wire transfers is an expeditious method of transferring the bank accounts. Wire transfers include transactions occurring within the national foundries of a country or from one country to another. Wire transfers do not involve actual movement of money. They are considered rapid as secured method for transferring value from one location to another.

- The branches of the Janata Co-operative Bank Ltd. may undertake domestic wire transfers only subject to the following conditions :
  - i. Information accompanying all domestic wire transfers of Rs.50000/- (Rupees Fifty Thousand) and above must include complete originator information i.e. name, address and account number etc., unless full originator information can be made available to the beneficiary bank by other means.
  - ii. If a bank has reason to believe that a customer is intentionally structuring wire transfer to below Rs.50,000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the bank must insist on complete customer identification before effecting the transfer. In case of non-cooperation from the customer, efforts should be made to establish his identity and Suspicious Transaction Report (STR) should be made to FIU-IND.
  - iii. When a credit or debit card is used to effect money transfer, necessary information as at (i) above should be included in the message.

#### **exemptions**

Interbank transfers and settlements where both the originator and beneficiary are banks or financial institutions would be exempted from the above requirements.

#### **42. Issue and Payment of Demand Drafts, etc.,**

Any remittance of funds by way of demand draft, mail/telegraphic transfer/NEFT/IMPS or any other mode and issue of travelers' cheques for value of rupees fifty thousand and above shall be effected by debit to the customer's accountor against cheques and not against cash payment.

Further, the name of the purchaser shall be incorporated on the face of the demand draft, pay order, banker's cheque, etc., by the issuing bank. These instructions shall take effect for such instruments issued on or after September 15, 2018.

#### 43. Quoting of PAN

Permanent account number (PAN) of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B applicable to banks, as amended from time to time. Form 60 shall be obtained from persons who do not have PAN.

#### 44. Selling Third party products

Bank acting as agents while selling third party products as per regulations in force from time to time shall comply with the following aspects for the purpose of these directions:

- i. the identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand as required under Section 13(e) of this Directions.
- ii. transaction details of sale of third party products and related records shall be maintained as prescribed in Chapter VII Section 46.
- iii. AML software capable of capturing, generating and analysing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.
- iv. transactions involving rupees fifty thousand and above shall be undertaken only by:
  - a) debit to customers' account or against cheques; and
  - b) obtaining and verifying the PAN given by the account based as well as walk-in customers.
- v. Instruction at 'd' above shall also apply to sale of Banks own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for rupees fifty thousand and above.

#### 45. At-par cheque facility

- i. Bank have arrangements with HDFC bank Ltd. under use the cheque book facility to issue 'at par' cheques to its constituents and walk-in- customers for effecting their remittances and payments. Since the 'at par' cheque facility offered by HDFC Bank Ltd. is in the nature of correspondent banking arrangement, branch should monitor and review such arrangements to assess the risks including credit risk and reputational risk arising therefrom. For this purpose, branch should retain the right to verify the records maintained of client branch for compliance with the extant instructions on KYC and AML under such arrangements.

In this regard, branches are advised to utilize the 'at par' cheque facility only for the following purposes:

- a) For their own use.
  - b) For their account holders who are KYC complaint provided that all transactions of Rs.50,000/- or more should be strictly by debit to the customer's account.
  - c) For walk-in customers against cash for less than Rs.50,000/- per individual.
- ii. In order to utilise the 'at par' cheque facility in the above manner, branches should maintain the following:
    - a) Records pertaining to issuance of 'at par' cheques covering inter alia applicant's name and account number, beneficiary's details and date of issuance of the 'at par' cheque.
    - b) Sufficient balances/drawing arrangements with the commercial bank extending such facility for purpose of honouring such instruments.

Branches should also ensure that all 'at par' cheques issued by them are crossed 'account payee' irrespective of the amount involved.

#### **46. Hiring of Employees and Employee training**

- i. Adequate screening mechanism as an integral part of their personnel recruitment/hiring process shall be put in place.
- ii. Bank shall endeavour to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. Bank shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.
- iii. On-going employee training programme shall be put in place so that the members of staff are adequately trained in AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the bank, regulation and related issues shall be ensured.

#### **47. Penalty for non compliance**

- i. Section 13 of the Prevention of Money Laundering Act, 2002 confers following powers on the Director, FIU-IND to ensure compliance.
  - a) The Director may, either of his own motion or on an application made by any authority, officer or person, make such inquiry or cause such inquiry to be made, as he thinks fit to be necessary, with regard to the obligations of the reporting entity, under this Chapter.
  - b) If at any stage of inquiry or any other proceedings before him, the Director having regard to the nature and complexity of the case, is of the opinion that it is necessary to do so, he may direct the concerned reporting entity to get its records, as may be specified, audited by an accountant from amongst a panel of accountants, maintained by the Central Government for this purpose.
  - c) The expenses of, and incidental to, any audit under sub-section (1A) shall be borne by the Central Government.
  - d) If the Director, in the course of any inquiry, finds that a reporting entity or its designated director on the Board or any of its employees has failed to comply with the obligations under this Chapter, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may-
    - (i) Issue a warning in writing; or
    - (ii) direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; or
    - (iii) direct such reporting entity or its designated director on the Board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or
    - (iv) by an order, impose a monetary penalty on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure.
  - e) The Director shall forward a copy of the order passed under sub-section (2) to every Banking Company, Financial Institution or Intermediary or person who is a party to proceeding under that sub-section.



## ii. General Guidelines

### a) Confidentiality of customer information:

Branches are advised that Information collected from customers for the purpose of opening of account is to be treated as confidential and details thereof should not be divulged for the purpose of cross selling, etc. Information sought from the customer should be relevant to the perceived risk and be non-intrusive. Any other information that is sought from the customer should be called for separately only after the account has been opened, with his/her express consent and in a different form, distinctly separate from the application form. It should be indicated clearly to the customer that providing such information is optional.

### b) Adherence to Know Your Customer (KYC) guidelines.

#### Avoiding hardship to customers:

Branches should keep in mind the spirit of the instructions issued by the Reserve Bank/Head Office so as to avoid undue hardships to individuals who are otherwise classified as low risk customers.

### c) Concurrent Auditor

To verify and record his comments on the effectiveness of measures taken by branches/ level of implementation of KYC guidelines.

## iii. Modifications/Additions in Policy.

Any modification/addition in the KYC Policy will be taken up and review to effect and incorporate changes, arising as result of changes in monetary fiscal & regulatory policy of the Government of India, Reserve Bank of India & Registrar of Co-operative Societies from time to time. It is clarified that bank will endeavor to meticulously adhere to the provisions of the master circular Know Your Customers(KYC) Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016, Master Circular No. DBR.AML.BC.No.15/14.01.001/2015-16 dated July 1, 2016 and DCBR.BPD (PCB) MC.No.6/13.01.000/2015-16 dated 01.07.2015 and amendment to Master Circular No.DOR.AML.REC.13/14.01.001/2023-24 dated May 4, 2023 as updated from time to time. An updated copy of the said direction will be provided to all the branches and their implementation will be closely monitored by the Inspection and Audit Compliance Sub-Committee which will submit periodically reports to the Management.

## 48. Conclusion.

This policy will be taken up for review as and when there are major changes in the environment arising out of changes in the KYC policy of Reserve Bank of India, fiscal policy of Government of India. However, in the absence of any such changes in the economic and banking scenario, this policy will continue to be in force. The changes made by the RBI and Government of India must be complied with and the Policy should be revised/rectified and amended accordingly. This policy has been framed and shall be valid till it is revised. It is clarified that bank will endeavor to meticulously adhere to the provisions of the master circular Know Your Customers(KYC) Master Circular No. DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016, Master Circular No. DBR.AML.BC.No.15/14.01.001/ 2015-16 dated July 1, 2016 and DCBR.BPD (PCB) MC.No.6/13.01.000/2015-16 dated 01.07.2015 and amendment to Master Circular No.DOR.AML.REC.13/14.01.001/2023-24 dated May 4, 2023 as updated from time to time. An updated copy of the said direction will be provided to all the branches and their implementation will be closely monitored by the Inspection and Audit Compliance Sub-Committee which will submit periodically reports to the Management.

## Annex I

### Government Order on Procedure for Implementation of Section 51A of The Unlawful Activities (Prevention) Act, 1967

File No.17015/10/2002-IS-VI

Government of India Ministry of Home Affairs Internal Security - I Division

New Delhi, Dated 27th August, 2009

To,

1. Governor, Reserve Bank of India, Mumbai
2. Chairman, Securities & Exchange Board of India, Mumbai
3. Chairman, Insurance Regulatory and Development Authority, Hyderabad
4. Foreign Secretary, Ministry of External Affairs, New Delhi
5. Finance Secretary, Ministry of Finance, New Delhi
6. Revenue Secretary, Department of Revenue, Ministry of Finance, New Delhi
7. Director, Intelligence Bureau, New Delhi
8. Additional Secretary, Department of Financial Services, Ministry of Finance, New Delhi
9. Chief Secretaries of all States / Union Territories

#### Order

#### **Procedure for Implementation of Section 51A of The Unlawful Activities (Prevention) Act, 1967**

The Unlawful Activities (Prevention) Act, 1967 (UAPA) was amended and notified on 31.12.2008, which, inter-alia, inserted Section 51A to the Act. Section 51A reads as under :

"51A. For the prevention of, and for coping with terrorist activities, the Central Government shall have power to -

- (a) freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities Listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism;
- (b) prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism;
- (c) prevent the entry into or the transit through India of individuals Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism",

#### **The Unlawful Activities (Prevention) Act define "Order" as under :**

"Order" means the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as may be amended from time to time.

In order to expeditiously and effectively implement the provisions of Section 51A, the

following procedures shall be followed :-

### **Appointment and Communication of Details of UAPA Nodal Officers**

2. As regards appointment and communication of details of UAPA nodal officers -

(i) The UAPA nodal officer for IS-I division would be the Joint Secretary (IS.I), Ministry of Home Affairs. His contact details are 011-23092736 (Tel), 011-23092569 (Fax) and [jsis@nic.in](mailto:jsis@nic.in) (e-mail id).

(ii) The Ministry of External affairs, Department of Economic affairs, Foreigners Division of MHA, FIU-IND; and RBI, SEBI, IRDA (hereinafter referred to as Regulators) shall appoint a UAPA nodal officer and communicate the name and contact details to the IS-I Division in MHA.

(iii) The States and UTs should appoint a UAPA nodal officer preferably of the rank of the Principal Secretary / Secretary, Home Department and communicate the name and contact details to the IS-I Division in MHA.

(iv) The IS-I Division in MHA would maintain the consolidated list of all UAPA nodal officers and forward the list to all other UAPA nodal officers.

(v) The RBI, SEBI, IRDA should forward the consolidated list of UAPA nodal officers to the Banks, stock exchanges / depositories, intermediaries regulated by SEBI and insurance companies respectively

(vi) The consolidated list of the UAPA nodal officers should be circulated to the nodal officer of IS-I Division of MHA in July every year and on every change. Joint Secretary (IS-I), being the nodal officer of IS-I Division of MHA, shall cause the amended list of UAPA nodal officers to be circulated to the nodal officers of Ministry of External Affairs, Department of Economic affairs, Foreigners Division of MHA, RBI, SEBI, IRDA and FIU-IND.

### **Communication of the List of Designated Individuals / Entities**

3. As regards communication of the list of designated individuals / entities -

(i) The Ministry of External Affairs shall update the list of individuals and entities subject to UN sanction measures on a regular basis. On any revision, the Ministry of External Affairs would electronically forward this list to the Nodal officers in Regulators, FIU-IND, IS-I Division and Foreigners' Division in MHA.

(ii) The Regulators would forward the list mentioned in (i) above (referred to as designated lists) to the banks, stock exchanges / depositories, intermediaries regulated by SEBI and insurance companies respectively.

(iii) The IS-I Division of MHA would forward the designated lists to the UAPA nodal officer of all States and UTs.

(iv) The Foreigners Division of MHA would forward the designated lists to the immigration authorities and security agencies.

**Regarding Funds, Financial Assets or Economic Resources or related Services held in the Form of Bank Accounts, Stocks or Insurance Policies etc.**

4. As regards funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or Insurance policies etc., the Regulators would forward the designated lists to the banks, stock exchanges / depositories, intermediaries regulated by SEBI and insurance companies respectively. The RBI, SEBI and IRDA would issue necessary guidelines to banks, stock exchanges / depositories, intermediaries regulated by SEBI and insurance companies requiring them to -
- (i) Maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether individuals or entities listed in the schedule to the Order, herein after, referred to as designated individuals / entities are holding any funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or Insurance policies etc., with them.
  - (ii) In case, the particulars of any of their customers match with the particulars of designated individuals / entities, the banks, stock exchanges / depositories, intermediaries regulated by SEBI and insurance companies shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or Insurance policies etc., held by such customer on their books to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: [jsis@nic.in](mailto:jsis@nic.in)
  - (iii) The banks, stock exchanges / depositories, intermediaries regulated by SEBI and insurance companies shall also send a copy of the communication mentioned in (ii) above to the UAPA nodal officer of the state / UT where the account is held and Regulators and FIU-IND, as the case may be.
  - (iv) In case, the match of any of the customers with the particulars of designated individuals / entities is beyond doubt, the banks, stock exchanges / depositories, intermediaries regulated by SEBI and insurance companies would prevent designated persons from conducting financial transactions, under intimation to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: [jsis@nic.in](mailto:jsis@nic.in)
  - (v) The Banks, stock exchanges / depositories, intermediaries regulated by SEBI and insurance companies, shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (ii) above, carried through or attempted as per the prescribed format.
5. On receipt of the particulars referred to in paragraph 3 (ii) above, IS-I Division of MHA would cause a verification to be conducted by the State Police and / or the Central Agencies so as to ensure that the individuals / entities identified by the Banks, stock exchanges / depositories, intermediaries regulated by SEBI and Insurance Companies are the ones listed as designated individuals / entities and the funds, financial assets or

economic resources or related services, reported by banks, stock exchanges / depositories, intermediaries regulated by SEBI and insurance companies are held by the designated individuals / entities. This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.

6. In case, the results of the verification indicate that the properties are owned by or are held for the benefit of the designated individuals / entities, an order to freeze these assets under section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned bank branch, depository, branch of insurance company branch under intimation to respective Regulators and FIU-IND. The UAPA nodal officer of IS-I Division of MHA shall also forward a copy thereof to all the Principal Secretary / Secretary, Home Department of the States or UTs, so that any individual or entity may be prohibited from making any funds, financial assets or economic resources or related services available for the benefit of the designated individuals / entities or any other person engaged in or suspected to be engaged in terrorism. The UAPA nodal officer of IS-I Division of MHA shall also forward a copy of the order under section 51A, to all Directors General of Police / Commissioners of Police of all states / UTs for initiating action under the provisions of Unlawful Activities (Prevention) Act.

The order shall take place without prior notice to the designated individuals / entities.

#### **Regarding Financial Assets or Economic Resources of the Nature of Immovable Properties**

7. IS-I Division of MHA would electronically forward the designated lists to the UAPA nodal officer of all States and UTs with the request to have the names of the designated individuals / entities, on the given parameters, verified from the records of the office of the Registrar performing the work of registration of immovable properties in their respective jurisdiction.
8. In case, the designated individuals / entities are holding financial assets or economic resources of the nature of immovable property and if any match with the designated individuals / entities is found, the UAPA nodal officer of the state / UT would cause communication of the complete particulars of such individual / entity along with complete details of the financial assets or economic resources of the nature of immovable property to Joint Secretary (IS.I), Ministry of Home Affairs, immediately within 24 hours at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post would necessarily be conveyed on e-mail id: [jsis@nic.in](mailto:jsis@nic.in).
9. The UAPA nodal officer of the state / UT may cause such inquiry to be conducted by the State Police so as to ensure that the particulars sent by the Registrar performing the work of registering immovable properties are indeed of these designated individuals / entities. This verification would be completed within a maximum of 5 working days and should be conveyed within 24 hours of the verification, if it matches with the particulars of the designated individual / entity to Joint Secretary (IS-I), Ministry of Home Affairs at the Fax, telephone numbers and also on the e-mail id given below.
10. A copy of this reference should be sent to Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011- 23092736.

The particulars apart from being sent by post would necessarily be conveyed on e-mail id: [jsis@nic.in](mailto:jsis@nic.in). MHA may have the verification also conducted by the Central Agencies. This verification would be completed within a maximum of 5 working days.

11. In case, the results of the verification indicate that the particulars match with those of designated individuals / entities, an order under section 51A of the UAPA would be issued within 24 hours, by the nodal officer of IS-I Division of MHA and conveyed to the concerned Registrar performing the work of registering immovable properties and to FIU-IND under intimation to the concerned UAPA nodal officer of the state / UT.

The order shall take place without prior notice, to the designated individuals / entities.

12. Further, the UAPA nodal officer of the state / UT shall cause to monitor the transactions / accounts of the designated individual / entity so as to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism. The UAPA nodal officer of the state / UT shall upon coming to his notice, transactions and attempts by third party immediately bring to the notice of the DGP / Commissioner of Police of the State / UT for also initiating action under the provisions of Unlawful Activities (Prevention) Act.

#### **Implementation of Requests Received from Foreign Countries under U.N. Security Council Resolution 1373 of 2001**

13. U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.
14. To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the UAPA nodal officer for IS-I Division for freezing of funds or other assets.
15. The UAPA nodal officer of IS-I Division of MHA, shall cause the request to be examined, within 5 working days, so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the nodal officers in Regulators, FIU-IND and to the nodal officers of the States / UTs. The proposed designee, as mentioned above would be treated as designated individuals / entities.

16. Upon receipt of the requests by these nodal officers from the UAPA nodal officer of IS-I Division, the procedure as enumerated at paragraphs 4 to 12 above shall be followed.

The freezing orders shall take place without prior notice to the designated persons involved

**Procedure for Unfreezing of Funds, Financial Assets or Economic Resources or related Services of Individuals / Entities Inadvertently affected by the Freezing Mechanism upon Verification that the Person or Entity is not a Designated Person**

17. Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned / held by them has been inadvertently frozen, they shall move an application giving the requisite evidence, in writing, to the concerned bank, stock exchanges / depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties and the State / UT nodal officers.
18. The banks, stock exchanges / depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties and the State / UT nodal officers shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the nodal officer of IS-I Division of MHA as per the contact details given in paragraph 4 (ii) above, within two working days.
19. The Joint Secretary (IS-I), MHA, being the nodal officer for IS-I Division of MHA shall cause such verification as may be required on the basis of the evidence furnished by the individual / entity and if he is satisfied, he shall pass an order, within 15 working days, unfreezing the funds, financial assets or economic resources or related services, owned / held by such applicant, under intimation to the concerned bank, stock exchanges / depositories, intermediaries regulated by SEBI, insurance company and the nodal officers of States / UTs. However, if it is not possible for any reason to pass an Order unfreezing the assets within 15 working days, the nodal officer of IS-I Division shall inform the applicant.

**Communication of Orders under Section 51A of Unlawful Activities(Prevention) Act**

20. All Orders under section 51A of Unlawful Activities (Prevention) Act, relating to funds, financial assets or economic resources or related services, would be communicated to all the banks, depositories / stock exchanges, intermediaries regulated by SEBI, insurance companies through respective Regulators, and to all the Registrars performing the work of registering immovable properties, through the state / UT nodal officer by IS-I Division of MHA.

**Regarding Prevention of Entry into or Transit through India**

21. As regards prevention of entry into or transit through India of the designated individuals, the Foreigners Division of MHA, shall forward the designated lists to the immigration authorities and security agencies with a request to prevent the entry into or the transit through India. The order shall take place without prior notice to the designated individuals / entities.

22. The immigration authorities shall ensure strict compliance of the Orders and also communicate the details of entry or transit through India of the designated individuals as prevented by them to the Foreigners' Division of MHA.

**Procedure for Communication of Compliance of Action taken under Section 51A**

23. The nodal officers of IS-I Division and Foreigners Division of MHA shall furnish the details of funds, financial assets or economic resources or related services of designated individuals / entities frozen by an order, and details of the individuals whose entry into India or transit through India was prevented, respectively, to the Ministry of External Affairs for onward communication to the United Nations.
24. All concerned are requested to ensure strict compliance of this order.



**Annex II**  
**KYC documents for eligible FPIs under PIS**

Document Type		FPI Type		
		Category I	Category II	Category III
Entity Level	Constitutive Documents (Memorandum and Articles of Association, Certificate of Incorporation etc.)	Mandatory	Mandatory	Mandatory
	Proof of Address	Mandatory (Power of Attorney {PoA} mentioning the address is acceptable as address proof)	Mandatory (Power of Attorney mentioning the address is acceptable as address proof)	Mandatory other than Power of Attorney
	PAN <sup>33</sup>	Mandatory	Mandatory	Mandatory
	Financial Data	Exempted *	Exempted *	Mandatory
	SEBI Registration Certificate	Mandatory	Mandatory	Mandatory
	Board Resolution@@	Exempted *	Mandatory	Mandatory
Senior Management (Whole Time Directors/ Partners/ Trustees/ etc.)	List	Mandatory	Mandatory	Mandatory
	Proof of Identity	Exempted *	Exempted *	Entity declares* on letter head full name, nationality, date of birth or submits photo identity proof
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *

Authorized Signatories	List and Signatures	Mandatory – list of Global Custodian signatories can be given in case of PoA to Global Custodian	Mandatory - list of Global Custodian signatories can be given in case of PoA to Global Custodian	Mandatory
	Proof of Identity	Exempted *	Exempted *	Mandatory
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *
Ultimate Beneficial Owner (UBO)	List	Exempted *	Mandatory (can declare “no UBO over 25%”)	Mandatory
	Proof of Identity	Exempted *	Exempted *	Mandatory
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *

\* Not required while opening the bank account. However, FPIs concerned may submit an undertaking that upon demand by Regulators/Law Enforcement Agencies the relative document/s would be submitted to the bank.

@@ FPIs from certain jurisdictions where the practice of passing Board Resolution for the purpose of opening bank accounts etc. is not in vogue, may submit ‘Power of Attorney granted to Global Custodian/Local Custodian in lieu of Board Resolution’

Category	Eligible Foreign Investors
I.	Government and Government related foreign investors such as Foreign Central Banks, Governmental Agencies, Sovereign Wealth Funds, International/ Multilateral Organizations/ Agencies.
II.	<ul style="list-style-type: none"> <li>a) Appropriately regulated broad based funds such as Mutual Funds, Investment Trusts, Insurance /Reinsurance Companies, Other Broad Based Funds etc.</li> <li>b) Appropriately regulated entities such as Banks, Asset Management Companies, Investment Managers/Advisors, Portfolio Managers etc.</li> <li>c) Broad based funds whose investment manager is appropriately regulated.</li> <li>d) University Funds and Pension Funds.</li> <li>e) University related Endowments already registered with SEBI as FII/Sub Account.</li> </ul>

III.	All other eligible foreign investors investing in India under PIS route not eligible under Category I and II such as Endowments, Charitable Societies/Trust, Foundations, Corporate Bodies, Trusts, Individuals, Family Offices, etc.
------	---

The Janata Co-operative Bank Ltd.